Webアプリケーションセキュリティ強化ガイド

この資料は、Webアプリケーションの安全性を高めるための8つの重要なチェック項目と、実作業に落とし込める指針をまとめたものです。さらに、WAF（Web Application Firewall）に関する情報も記載しています。

【チェックリストと指針】

1. 入力検証・認証強化

サーバ側でホワイトリスト検証を実施し、MFA（多要素認証）を必須化してください。

2. セッション管理

セッションIDを安全に生成し、HTTPSを強制、タイムアウトを設定してください。

3. 暗号化とデータ保護

TLS1.2以上を使用し、AES256で暗号化、鍵管理ポリシーを策定してください。

4. セキュリティヘッダー設定

X-Frame-Options、CSP、X-XSS-Protectionなどのヘッダーを設定してください。

5. WAF導入

**AWS WAFやCloudflare
WAFなどを導入し、SQLインジェクションやXSS対策ルールを有効化してください。**

6. OWASP Top 10準拠

脆弱性レビューを実施し、開発プロセスにセキュリティテストを組み込んでください。

7. 監視・インシデント対応

SIEMでログを集中管理し、異常検知時には即時対応できる体制を整えてください。

8. バックアップ戦略

暗号化バックアップをオフサイトに保管し、定期的に復旧テストを行ってください。

**【WAFに関する情報】
以下のサービスを利用することで、Webアプリケーションの防御を強化できます。 - AWS WAF: https://aws.amazon.com/waf/ - Cloudflare WAF: https://www.cloudflare.com/waf/ - Azure WAF: https://azure.microsoft.com/en-us/services/web-application-firewall/**